Trusted Solaris System Administration using Sun Ray Ultra Thin Client Technology

Who Can Benefit

Trusted Solaris 8 OS system administrators and network administrators responsible for understanding and administering Trusted Solaris in an environment that includes Sun Ray ultra-thin client technology.

Prerequisites : **To succeed fully in this course, students should be able to:**
- Add and delete users
- Share file systems and directories
- Install and configure custom software, including the Solaris OS

Skills Gained : **Upon completion of this course, you should be able to:**
- Administer Trusted Solaris in an environment that includes Sun Ray ultra-thin clients
- Describe the Trusted Solaris OS access control and labels
- Work within the Trusted Solaris OS Common Desktop Environment (CDE)
- Work with labeled data
- Configure Trusted Solaris OS based upon security requirements
- Add users within the Trusted Solaris OS
- Establish privileges
- Process authorization, attributes, and execution profiles
- Configure Trusted Solaris OS networking aspects
- Manage devices and file systems
- Install and configure the Trusted Solaris OS
- Describe auditing and analyze audit trails

Related Courses
- **Before:** SA-239: Intermediate System Administration for the Solaris 9 Operating System
- **After:** SC-300: Administrating Security on Solaris 2.X Environments

Course Content

Module 1: Trusted Solaris OS Concepts
- Describe the Common Criteria standards for evaluating information technology (IT) security
- Select an operating system security structure that fits with your local site's security policy
- Explain how the Trusted Solaris OS can satisfy your company's security requirements

Module 2: Access Control and Labels
- Use the Discretionary Access Control (DAC) features
- Use the Mandatory Access Control (MAC) components and features
- Describe the interaction of DAC and MAC as part of the implementation of the security policy

Module 3: Solaris Management Console
- Describe how to use the Trusted Solaris Management Console (SMC)
- Initialize and configure databases
- Manage users, roles, and hosts

Module 4: Accessing a Trusted Solaris OS
- Log in to a Trusted Solaris OS
- Identify the features of Trusted CDE
- Work within the Trusted Solaris OS windowing environment
- Create workspaces with different sensitivity labels

Module 5: The Trusted Window Environment
- Describe the CDE environment and the MAC extensions to it
- Use ACLs on files and directories
- Use multilevel directories
- Use the drag-and-drop and copy-and-paste features of the Trusted Solaris OS
- Use and describe the handling of email, calendars, and other features on systems running the Trusted Solaris OS

Module 6: The label_encodings Database
- Describe the concepts of the label_encodings database and the role it plays in setting security policy
- Demonstrate through examples the steps to create, test, and implement a label_encodings database
- Analyze an existing label_encodings database, explaining the sections and their function and importance

Module 7: Privileges and Process Attributes
- Describe the advantages of the Principle of Least Privilege from a technical point of view
- Check and assign privileges to an application
- Verify what privileges are needed by an application in order to run successfully

Module 8: User and Role Authorizations and Rights Profiles
- Describe authorizations and how they are applied to users and roles with the use of rights profiles
- Choose the right profile to assign to a user
- Create new rights profiles and modify existing ones

Module 9: Configuring the Network
- Differentiate between the various networking protocols supported by the Trusted Solaris OS
- Properly configure the networking aspects of the Trusted Solaris OS

Module 10: Device and File System Management
- Configure file systems, including disk-based and NFS
- Configure and use allocatable devices and printers

Module 11: JumpStart and Name Services
- List the primary components for setting up a JumpStart network installation
- Set up a JumpStart installation server to provide the Trusted Solaris OS with the software necessary to install clients from a workstation running the standard Solaris OS
- Add install clients to the install servers and boot servers
- Create a configuration server with customized rules and class files
- Boot install clients
- Install and configure NIS+ and NIS

Module 12: Installation and Configuration
- Explain the hardware requirements for a Trusted Solaris OS installation
- State the different installation methods available for the Trusted Solaris OS
- Describe the differences between the installation of the Trusted Solaris OS and standard Solaris OS
- Install and configure a Workstation with the Trusted Solaris OS

Module 13: Audit Configuration
- Describe how the auditing system works, and be able to customize it so it will not bring your system to a halt
- Define what actions are to be audited
- Analyze the resulting audit trail

Module 14: Understanding Trusted Solaris on Sun Ray systems
- Sun Ray ultra-thin client technology overview
- Comparison between Sun Ray clients and other Desktop Systems
- Architecture
- Benefits of Sun Ray ultra-thin client technology
- Security limitations

Module 15: Installation and Administration of Trusted Solaris on Sun Ray systems
- Trusted Solaris system security toolkit
- Trusted guard
- Sun Ray ultra-thin client server
- Consolidated server

LAB: Installation of Trusted Solaris on the Sun Ray ultra-thin client